2022

Dumps Professor

ANS-C00 Dumps

AWS CERTIFIED ADVANCED NETWORKING SPECIALTY EXAM

VERSION: DEMO, TOTAL QUESTIONS: 10

https://www.dumpsprofessor.com/amazon/ans-c00-dumps-pdf

Question # 1

A company wants to migrate its production and development applications to the AWS Cloud across multiple VPCs in three AWS Regions us-east-1 (N Virginia), eu-west-1 (Ireland), and ap-southeast-1 (Singapore) The Company needs a scalable solution that provides connectivity between all three Regions The solution also must provide private connectivity to the company's on-premises data centre in Northern Virginia Data that is transferred from on premises and data that is transferred between Regions must be encrypted in transit The company requires predictable network performance and must minimize cost

The company has initiated a solution by deploying a transit gateway with two route tables in each Region One route table is for the production environment, and one route table is for the development environment

What else must the company do to meet its requirements with the LOWEST latency?

A. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data centre on each transit gateway, create a VPN attachment over the public VIF for the production and development route tables Create transit gateway peennng connections to route traffic between Regions.

B. Deploy an AWS Direct Connect connection in us-east-1 and a transit VIF to the on-premises data centre Associate all transit gateways and the transit VIF with a different Direct Connect gateway. Create transit gateway peering connections to route traffic between Regions.

C. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center. On each transit gateway, create a VPN attachment over the public VIF for the production and development route tables. Route traffic between Regions through the VPN connections.

D. Deploy an AWS Direct Connect connection in us-east-1 to the on-premises data center Create one transit VIF for each transit gateway route table, and associate each transit VIF with a Direct Connect gateway Associate all transit gateways with the Direct Connect gateway Create transit gateway peering connections to route traffic between Regions.

Answer: A

Question # 2

A company needs to allow its remote users to access company resources in the AWS Cloud. The company has two VPCs that are connected through VPC peering. The remote users must be able to access resources in both VPCs by using secure connections from their laptop computers The Company does not want to implement an access management solution that requires additional costs or effort. Which solution meets these requirements?

A. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target network. Add a rule to authorize client access to the target VPC. and add a rule to authorize client access to the peered VPC. Update resource security groups in both VPCs to allow traffic from the security group for the subnet association. Instruct the users to sign in to the AWS Management Console and navigate to Client VPN to connect to the Client VPN endpoint.

B. Deploy an AWS Client VPN endpoint in both VPCs, associate subnets, and define a target network. Add a rule to authorize client access to each target VPC. Update resource security groups in both VPCs to allow traffic from the security groups of each VPC for the subnet associations. Securely send the users the configuration options, and instruct the users to install Client VPN endpoints at the same time to gain access to the resources.

C. Deploy a Network Load Balancer in front of the company resources. Set up security groups that contain the IP addresses of each of the user laptops. Instruct the users to connect to the application securely over TCP.

D. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target network. Add a rule to authorize client access to the target VPC. and add a rule to authorize client access to the peered VPC. Update resource security groups in both VPCs to allow traffic from the security group for the subnet association. Securely send the users the configuration options, and instruct the users to install Client VPN on their laptops. Instruct the users to connect to the Client VPN endpoint to gain access to the resources.

Answer: B

Question # 3

You are deploying an EC2 instance in a private subnet that requires access to the Internet. One of the requirements for this solution is to restrict access to only particular URLs on a whitelist. In addition to the whitelisted URL, the instances should be able to access any Amazon S3 bucket in the same region via any URL.

Which of the following solutions should you deploy? (Select two.)

A. **Include s3.amazonaws.com in the whitelist.**

B. **Create a VPC endpoint for S3.**

C. **Run Squid proxy on a NAT instance.**

D. **Deploy a NAT gateway into your VPC.**

E. **Utilize a security group to restrict access.**

Answer: B C

Question # 4

An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used. Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: "There are not enough free addresses in subnet 'subnet-12345677' to satisfy the requested number of instances."

What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.

B. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CIDR. Include the new subnet in the Auto Scaling group.

C. Resize the IPv6 CIDR on each of the existing subnets. Modify the Auto Scaling group maximum number of instances.

D. Add a secondary IPv4 CIDR to the Amazon VPC. Assign secondary IPv4 address space to each of the existing subnets.

Answer: B

Question # 5

A company installed an AWS Site-to-Site VPN and configured it to use two tunnels The company has learned that the VPN connectivity is unstable During a ping test from the on-premises data center to AWS: a network engineer notices that the first few ICMP replies time out but that subsequent requests are successful The AWS Management Console shows that the status for both tunnels last changed at the same time the ping responses were successfully received

Which steps should the network engineer take to resolve the instability*? (Select TWO)

A. **Enable dead peer detection (DPD) on the customer gateway device**

B. **Change the tunnel configuration to active/standby on the virtual private gateway**

C. **Use AS PATH prepending on one path to cause all traffic to prefer that tunnel**

D. **Send ICMP requests to an instance in the VPC every 5 seconds from the on-premises network**

E. **Use a higher multi-exit discriminator (MED) value on the preferred path to prefer that tunnel**

Answer: A D